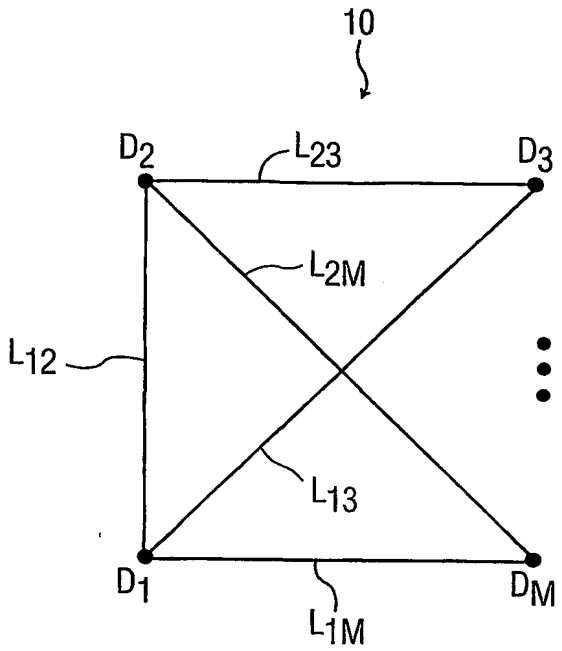

FIG. 1

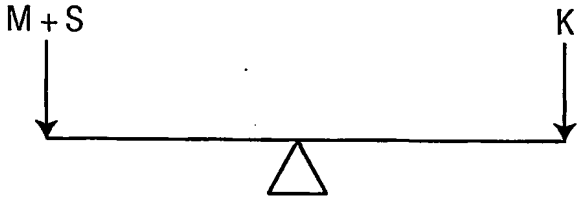

FIG. 2

NETWORK NODE (DEVICE)

NETWORK DATA STRUCTURE, INITIALLY EMPTY	
PUBLIC - PRIVATE KEY PAIR - OR OTHER SECURE, AUTHENTICATED MEANS OF COMMUNICATION (E.G., IEEE 1394)	
TOKEN COUNTER	
CONTENT MEMORY	
CAPABILITY FLAGS	CAN DEVICE JOIN OTHER DEVICES?
	CAN DEVICE STORE CONTENT?
	CAN DEVICE TRANSMIT CONTENT?
	USES PUBLIC KEY OR GLOBAL KEY ENCRYPTION?
CONTROLLER	

FIG. 3

NETWORK DATA STRUCTURE

NETWORK SIZE CONSTANT, K (10 TO 30)
CREATION DATE, TIME
NETWORK ID (128 BIT)
ENCRYPTION KEY (128 BIT)
DECRYPTION KEY (128 BIT)
GLOBAL REVOCATION LIST (OF COMPROMISED, ROGUE DEVICES) - RECEIVED FROM OUTSIDE
LOCAL REVOCATION LIST (OF COMPROMISED, ROGUE DEVICES) - DISCOVERED, INPUT IN THE NETWORK

FIG. 4

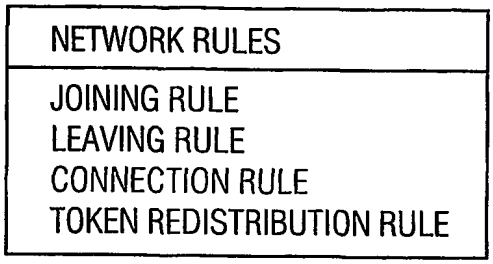
NETWORK RULES
JOINING RULE
LEAVING RULE
CONNECTION RULE
TOKEN REDISTRIBUTION RULE

FIG. 5

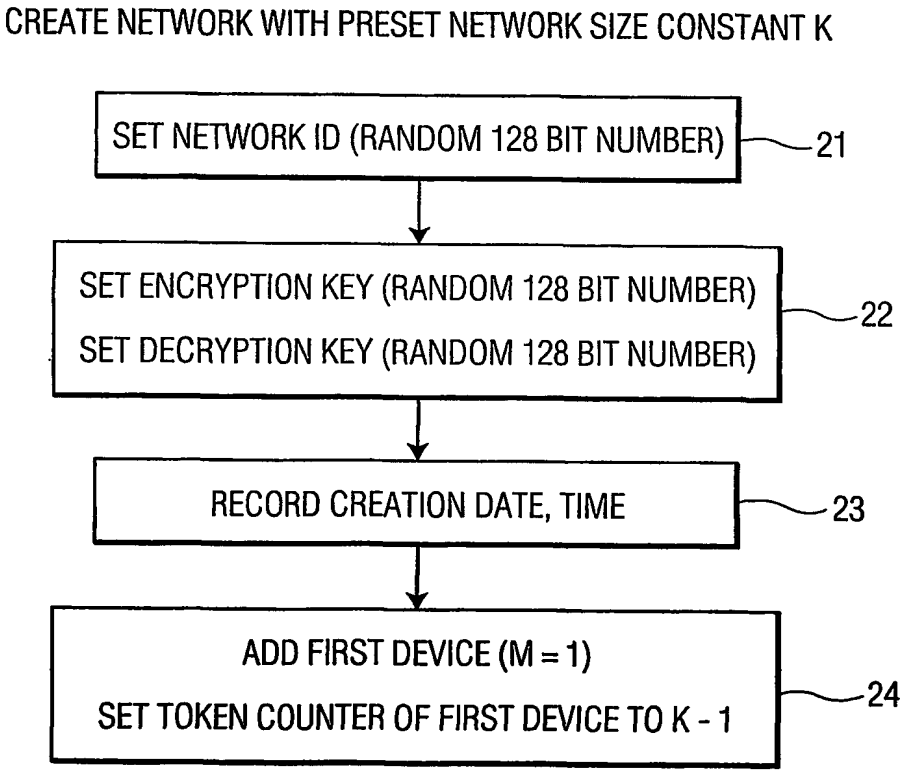
CREATE NETWORK WITH PRESET NETWORK SIZE CONSTANT K
SET NETWORK ID (RANDOM 128 BIT NUMBER)
21
SET ENCRYPTION KEY (RANDOM 128 BIT NUMBER)
SET DECRYPTION KEY (RANDOM 128 BIT NUMBER)
22
RECORD CREATION DATE, TIME
23
ADD FIRST DEVICE (M = 1)
SET TOKEN COUNTER OF FIRST DEVICE TO K - 1
24

FIG. 6

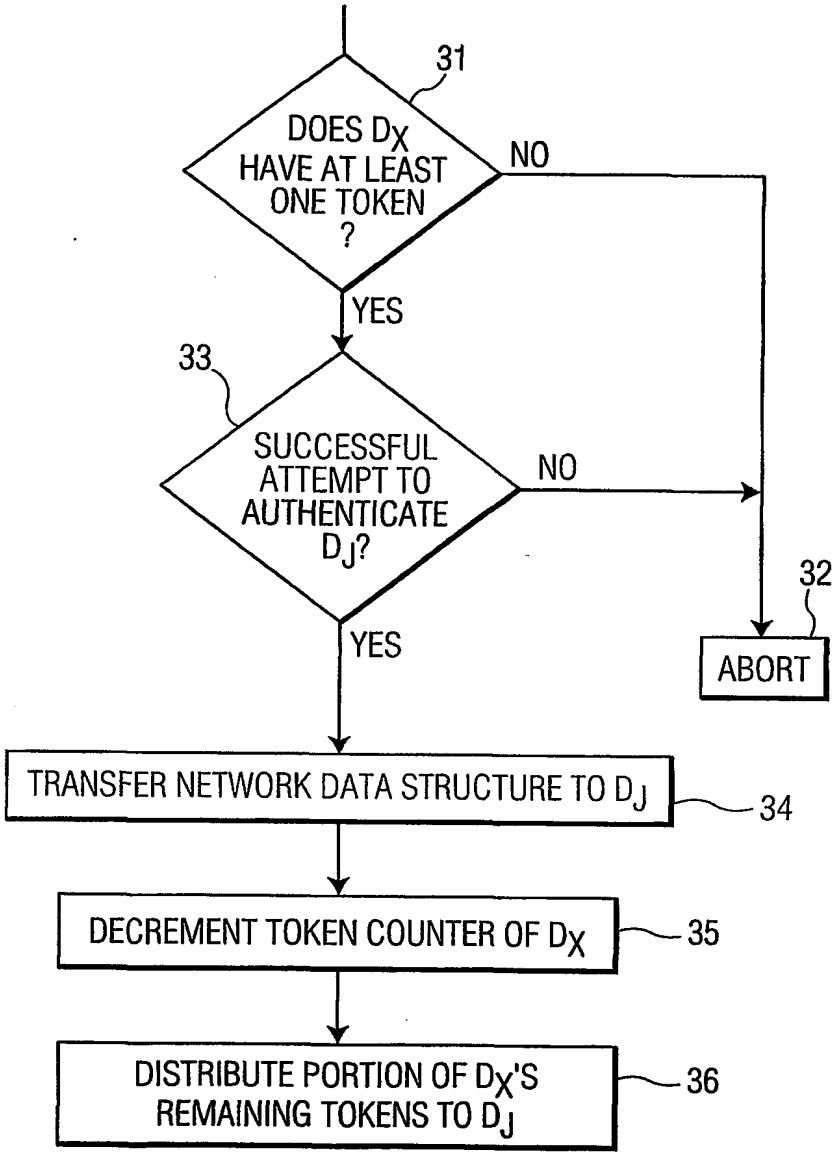
31
DOES D_X HAVE AT LEAST ONE TOKEN ?
NO
YES
33
SUCCESSFUL ATTEMPT TO AUTHENTICATE D_J?
NO
YES
32
ABORT
TRANSFER NETWORK DATA STRUCTURE TO D_J
34
DECREMENT TOKEN COUNTER OF D_X
35
DISTRIBUTE PORTION OF D_X'S REMAINING TOKENS TO D_J
36

FIG. 7

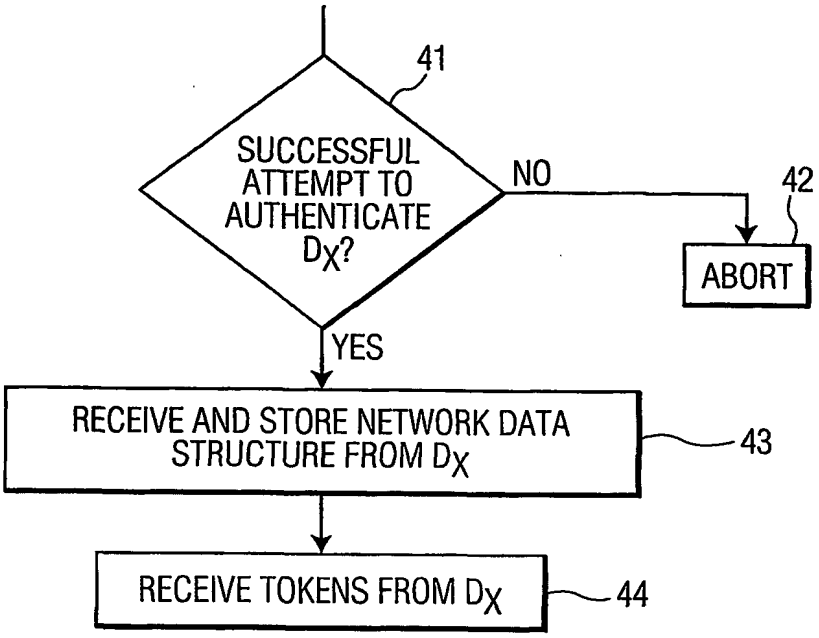
41
SUCCESSFUL ATTEMPT TO AUTHENTICATE D_X?
NO
42
ABORT
YES
RECEIVE AND STORE NETWORK DATA STRUCTURE FROM D_X
43
RECEIVE TOKENS FROM D_X
44

FIG. 8

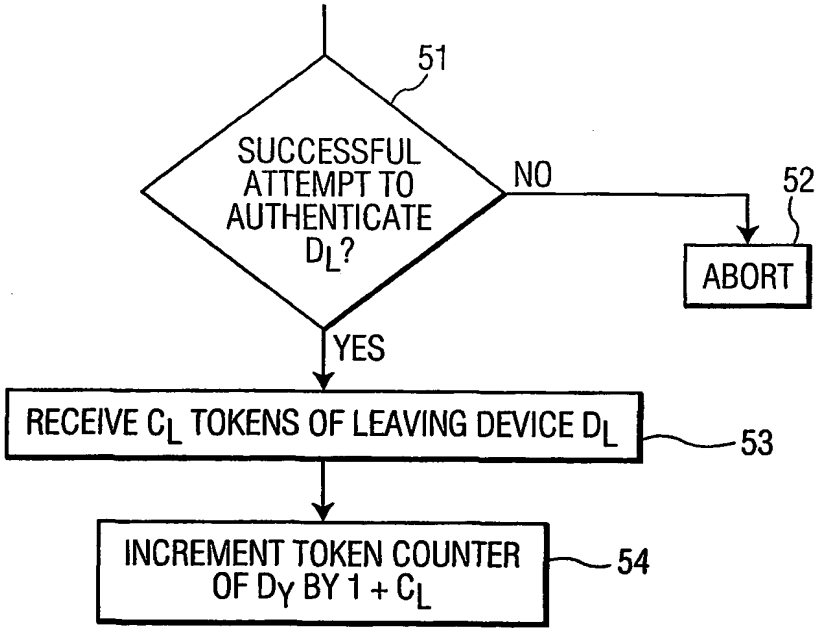
51
SUCCESSFUL ATTEMPT TO AUTHENTICATE D_L?
NO
52
ABORT
YES
RECEIVE C_L TOKENS OF LEAVING DEVICE D_L
53
INCREMENT TOKEN COUNTER OF D_Y BY 1 + C_L
54

FIG. 9

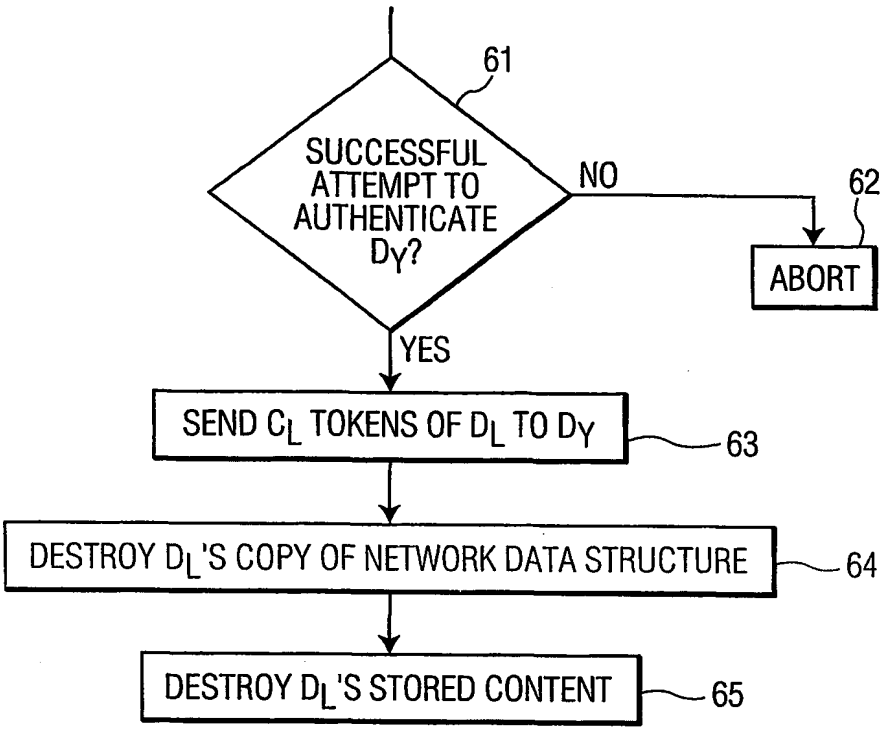
61
SUCCESSFUL ATTEMPT TO AUTHENTICATE D_Y?
NO
62
ABORT
YES
SEND C_L TOKENS OF D_L TO D_Y
63
DESTROY D_L'S COPY OF NETWORK DATA STRUCTURE
64
DESTROY D_L'S STORED CONTENT
65

FIG. 10

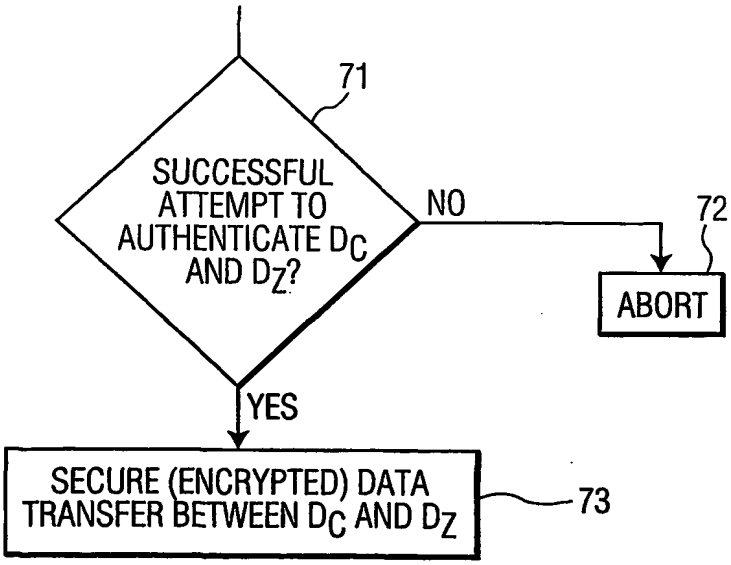
71
SUCCESSFUL ATTEMPT TO AUTHENTICATE D_C AND D_Z?
NO
72
ABORT
YES
SECURE (ENCRYPTED) DATA TRANSFER BETWEEN D_C AND D_Z
73

FIG. 11